

ON THE FERMAT-TYPE EQUATION $x^3 + y^3 = z^p$

NUNO FREITAS

ABSTRACT. We prove that the Fermat-type equation $x^3 + y^3 = z^p$ has no solutions (a, b, c) satisfying $abc \neq 0$ and $\gcd(a, b, c) = 1$ when -3 is not a square mod p . This improves to approximately 0.844 the Dirichlet density of the set of prime exponents to which the previous equation is known to not have such solutions.

For the proof we develop a criterion of independent interest to decide if two elliptic curves with certain type of potentially good reduction at 2 have symplectically or anti-symplectically isomorphic p -torsion modules.

1. INTRODUCTION

In this paper we consider the Fermat-type equation

$$(1.1) \quad x^3 + y^3 = z^p$$

which is a particular case of the *Generalized Fermat Equation* (GFE)

$$x^p + y^q = z^r, \quad p, q, r \in \mathbb{Z}_{\geq 2}, \quad 1/p + 1/q + 1/r < 1.$$

Here we are concerned with solutions (a, b, c) which are *non-trivial* and *primitive*, that is $abc \neq 0$ and $\gcd(a, b, c) = 1$, respectively. To the triple of exponents (p, q, r) we call the *signature* of the equation.

The equation (1.1) is one of the few instances of the GFE where there is a known Frey curve defined over \mathbb{Q} attached to it. The other few signatures with available rational Frey curves are (p, p, p) , $(p, p, 2)$, $(p, p, 3)$, $(5, 5, p)$, $(7, 7, p)$, $(2, 3, p)$ and $(4, p, 4)$ (see [3] for their explicit definitions).¹ However, only for the signatures (p, p, p) , $(4, p, 4)$, $(p, p, 2)$ and $(p, p, 3)$ the existence of a Frey curve led to a full resolution of the corresponding equation. The first due to the groundbreaking work of Wiles [17] and the other three due to work of Darmon [4] and Darmon-Merel [5]. Among the remaining signatures, equation (1.1) is the one where most progress was achieved so far, due to the work of Kraus [10] and Chen–Siksek [2].

Theorem 1 (Kraus 1998). *Let $p \geq 17$ be a prime and (a, b, c) be a non-trivial primitive solution to (1.1). Then $v_2(a) = 1$, $v_2(b) = 0$, $v_2(c) = 0$, and $v_3(c) \geq 1$.*

Moreover, there are no solutions for exponents p satisfying $17 \leq p < 10^4$.

Theorem 2 (Chen–Siksek 2009). *For a set of primes \mathcal{L} with density 0.681 the equation (1.1) has no non-trivial primitive solutions. The primes in \mathcal{L} are determined by explicit congruence conditions, for example $p \equiv 2, 3 \pmod{5}$.*

Date: January 26, 2016.

¹There are also Frey curves attached to signatures of the form (r, r, p) and $(2\ell, 2m, p)$ but defined over totally real fields (see [7] and [1]).

Moreover, there are no solutions for exponents p satisfying $3 \leq p \leq 10^7$.

In this work our main goal is to prove the following theorem.

Theorem 3. *Let $p \geq 17$ be a prime satisfying $(-3/p) = -1$, that is $p \equiv 2 \pmod{3}$. Then equation (1.1) has no non-trivial primitive solutions.*

Therefore, equation (1.1) has no non-trivial primitive solutions for a set of prime exponents with density approximately 0.844.

A crucial tool for the proof is the following criterion to decide whether two elliptic curves having certain type of potentially good reduction at 2 admit a symplectic or anti-symplectic isomorphism between their p -torsion modules (see beginning of Section 3 for the definitions).

Write \mathbb{Q}_2^{un} for the maximal unramified extension of \mathbb{Q}_2 .

Theorem 4. *Let E/\mathbb{Q}_2 and E'/\mathbb{Q}_2 be elliptic curves with potentially good reduction. Write $L = \mathbb{Q}_2^{un}(E[p])$ and $L' = \mathbb{Q}_2^{un}(E'[p])$. Write $\Delta_m(E)$ and $\Delta_m(E')$ for the minimal discriminant of E and E' respectively. Let $I_2 \subset \text{Gal}(\overline{\mathbb{Q}_2}/\mathbb{Q}_2)$ be the inertia group.*

Suppose that $L = L'$ and $\text{Gal}(L/\mathbb{Q}_2^{un}) \simeq \text{SL}_2(\mathbb{F}_3)$. Then, $E[p]$ and $E'[p]$ are isomorphic I_2 -modules for all prime $p \geq 3$. Moreover,

- (1) *if $(2/p) = 1$ then $E[p]$ and $E'[p]$ are symplectically isomorphic I_2 -modules.*
- (2) *if $(2/p) = -1$ then $E[p]$ and $E'[p]$ are symplectically isomorphic I_2 -modules if and only if $v_2(\Delta_m(E)) \equiv v_2(\Delta_m(E')) \pmod{3}$.*

This theorem extends the ideas in [9, Appendice A] and it is proved in Section 3; in Section 2 we use it to establish Theorem 3.

In [8] we develop further symplecticity criteria and apply them to the Generalized Fermat Equation $x^2 + y^3 = z^p$.

Idea behind the proof. Our proof of Theorem 3 builds on Kraus' modular argument [10]. Indeed, for $p \geq 17$ he attaches to a putative non-trivial primitive solution (a, b, c) of (1.1) a Frey elliptic curve

$$E_{a,b} : Y^2 = X^3 + 3abX + b^3 - a^3, \quad \Delta(E_{a,b}) = -2^4 \cdot 3^3 \cdot c^{2p}$$

and shows that its mod p Galois representation $\overline{\rho}_{E_{a,b},p}$ is mostly independent of (a, b, c) . By the now classic modularity, irreducibility and level lowering results over \mathbb{Q} it follows that $\overline{\rho}_{E_{a,b},p}$ is isomorphic to $\overline{\rho}_{f,p}$ the mod \mathfrak{p} representation attached to a rational newform f in a finite list. Finally, among all the possibilities for f Kraus obtains a contradiction except for the newform corresponding to the rational elliptic curve with Cremona label 72a1.

In particular, following the ideas in [14], Kraus' work implies that the solution (a, b, c) gives rise to a rational point on one of the modular curves $X_{72a1}^+(p)$ or $X_{72a1}^-(p)$; these curves respectively parameterize elliptic curves with p -torsion modules symplectically or anti-symplectically isomorphic to the p -torsion module of 72a1. By applying Theorem 4 and [12, Proposition 2] we will show that there are no 2-adic points in $X_{72a1}^-(p)$ and 3-adic points in $X_{72a1}^{(-3/p)}(p)$ arising from relevant solutions of (1.1). In particular, when $(-3/p) = -1$ this implies there are no relevant points on $X_{72a1}^\pm(p)(\mathbb{Q})$.

Acknowledgments. I would like to thank Benjamin Matschke, Bartosz Naskręcki and Michael Stoll for helpful discussions. I also thank Alain Kraus for his comments.

2. PROOF OF THEOREM 3

Let (a, b, c) be a non-trivial primitive solution to $x^3 + y^3 = z^p$. From Theorem 1 we know that $v_2(a) = 1$, $v_2(b) = 0$, $v_2(c) = 0$ and $v_3(c) \geq 1$ and we can attach to it the Frey curve

$$E_{a,b} : Y^2 = X^3 + 3abX + b^3 - a^3.$$

A closer look into Kraus' proof shows also that the mod p Galois representation of $E_{a,b}$ has to satisfy $\bar{\rho}_{E_{a,b},p} \sim \bar{\rho}_{W',p}$, where W' is the elliptic curve with Cremona label 72a1. Moreover, this possibility is the unique obstruction to conclude that (1.1) has no non-trivial primitive solutions. We shall show that $\bar{\rho}_{E_{a,b},p} \not\sim \bar{\rho}_{W',p}$ when $(-3/p) = -1$.

Note that W' has potentially multiplicative reduction at 3, which becomes multiplicative after twisting by -3 . Write E and W for the quadratic twists by -3 of $E_{a,b}$ and W' , respectively. Thus we have

$$(2.1) \quad \bar{\rho}_{E,p} \sim \bar{\rho}_{W,p},$$

where W has Cremona reference 24a4 with j -invariant $j_W = 2048/3$ and minimal model

$$W : Y^2 = X^3 - X^2 + X.$$

Since $v_2(j_W) = 11$ the curve W has potentially good reduction at 2 and it gets good reduction over $L = \mathbb{Q}_2^{un}(W[p])$. The curve W also satisfies

$$v_2(\Delta_m(W)) = 4 \quad \text{and} \quad v_2(c_4(W)) = 5,$$

hence $\text{Gal}(L/\mathbb{Q}_2^{un}) \simeq \text{SL}_2(\mathbb{F}_3)$ by [11]. From (2.1) the same must be true for E , therefore we are under the hypothesis of Theorem 4.

From part (2.2) in the proof of [10, Lemma 4.1] we have that $E_{a,b}$ is minimal at 2 and satisfies $v_2(\Delta_m(E_{a,b})) = 4$. Hence the same is true for the quadratic twist $E = -3E_{a,b}$ and we have $v_2(\Delta_m(E)) \equiv v_2(\Delta_m(W)) \pmod{3}$. We conclude from Theorem 4 that $E[p]$ and $W[p]$ are symplectically isomorphic I_2 -modules for all $p \geq 3$. Since $\bar{\rho}_{W,p}(I_2)$ is non-abelian, $E[p]$ and $W[p]$ are also symplectically isomorphic as $G_{\mathbb{Q}}$ -modules by [9, Lemma A.4]; moreover, they cannot be simultaneously symplectic and anti-symplectic isomorphic by Lemma 1.

From [12, Proposition 2] applied with the multiplicative prime $\ell = 3$ it follows that $E[p]$ and $W[p]$ are symplectically isomorphic if and only if $v_3(\Delta_m(W))$ and $v_3(\Delta_m(E))$ differ multiplicatively by a square modulo p . We now compute these quantities.

One easily checks that $v_3(\Delta_m(W)) = 1$.

From part (3.1) in the proof of [10, Lemma 4.1] we see that

$$v_3(c_4(E_{a,b})) = 2, \quad v_3(c_6(E_{a,b})) = 3, \quad v_3(\Delta(E_{a,b})) = 3 + 2pv_3(c).$$

Therefore, the twisted curve $E = -3E_{a,b}$ satisfies

$$v_3(c_4(E)) = 4, \quad v_3(c_6(E)) = 6, \quad v_3(\Delta(E)) = 9 + 2pv_3(c).$$

Since $v_3(c) \geq 1$ it follows from Table II in [13] that the equation for E is not minimal. After a change of variables we obtain

$$v_3(c_4) = 0, \quad v_3(c_6) = 0, \quad v_3(\Delta_m(E)) = -3 + 2pv_3(c)$$

and the model gets multiplicative reduction. Therefore, $E[p]$ and $W[p]$ are symplectically isomorphic if and only if

$$1 = v_3(\Delta_m(W)) \equiv u^2 v_3(\Delta_m(E)) = u^2(-3 + 2pv_3(c)) \pmod{p}$$

which is equivalent to $(-3/p) = 1$. The result follows.

The statement about the density follows by the same computations as in [2, Section 10] but now we also take into account the congruence $p \equiv 2 \pmod{3}$.

3. SYMPLECTIC ISOMORPHISMS OF THE p -TORSION OF ELLIPTIC CURVES

Let p be a prime. Let K be a field of characteristic zero or a finite field of characteristic $\neq p$ with an algebraic closure \overline{K} . Fix $\zeta_p \in \overline{K}$ a primitive p -th root of unity. For E an elliptic curve defined over K we write $E[p]$ for its p -torsion G_K -module, $\overline{\rho}_{E,p}: G_K \rightarrow \text{Aut}(E[p])$ for the corresponding Galois representation and $e_{E,p}$ for the Weil pairing on $E[p]$. We will call an \mathbb{F}_p -basis (P, Q) of $E[p]$ *symplectic* if $e_{E,p}(P, Q) = \zeta_p$.

Now let E/K and E'/K be two elliptic curves and $\phi: E[p] \rightarrow E'[p]$ be an isomorphism of G_K -modules. Then there is an element $r(\phi) \in \mathbb{F}_p^\times$ such that

$$e_{E',p}(\phi(P), \phi(Q)) = e_{E,p}(P, Q)^{r(\phi)} \quad \text{for all } P, Q \in E[p].$$

Note that for any $a \in \mathbb{F}_p^\times$ we have $r(a\phi) = a^2 r(\phi)$. We say that ϕ is a *symplectic isomorphism* if $r(\phi) = 1$ or, more generally, $r(\phi)$ is a square in \mathbb{F}_p^\times . Fix a nonsquare $r_p \in \mathbb{F}_p^\times$. We say that ϕ is a *anti-symplectic isomorphism* if $r(\phi) = r_p$ or, more generally, $r(\phi)$ is a nonsquare in \mathbb{F}_p^\times . Finally, we say that $E[p]$ and $E'[p]$ are *symplectically isomorphic* (or *anti-symplectically isomorphic*), if there exists a symplectic (or anti-symplectic) isomorphism of G_K -modules between them. Note that it is possible that $E[p]$ and $E'[p]$ are both symplectically and anti-symplectically isomorphic; this will be the case if and only if $E[p]$ admits an anti-symplectic automorphism.

We will need the following criterion.

Lemma 1. *Let E and E' be two elliptic curves defined over a field K with isomorphic p -torsion. Fix symplectic bases for $E[p]$ and $E'[p]$. Let $\phi: E[p] \rightarrow E'[p]$ be an isomorphism of G_K -modules and write M_ϕ for the matrix representing ϕ with respect to the fixed bases.*

Then ϕ is a symplectic isomorphism if and only if $\det(M_\phi)$ is a square mod p ; otherwise ϕ is anti-symplectic.

Moreover, if $\overline{\rho}_{E,p}(G_K)$ is a non-abelian subgroup of $\text{GL}_2(\mathbb{F}_p)$, then $E[p]$ and $E'[p]$ cannot be simultaneously symplectically and anti-symplectically isomorphic.

Proof. Let $P, Q \in E[p]$ and $P', Q' \in E'[p]$ be symplectic bases. We have that

$$e_{E',p}(\phi(P), \phi(Q)) = e_{E',p}(P', Q')^{\det(M_\phi)} = \zeta_p^{\det(M_\phi)} = e_{E,p}(P, Q)^{\det(M_\phi)},$$

so $r(\phi) = \det(M_\phi)$. This implies the first assertion.

We now prove the last statement. Let $\beta: E[p] \rightarrow E'[p]$ be another isomorphism of G_K -modules. Then $\beta^{-1}\phi = \lambda$ is in the centralizer of $\bar{\rho}_{E,p}(G_K)$. Since $\bar{\rho}_{E,p}(G_K)$ is non-abelian, λ is represented by a scalar matrix (see [9, Lemme A.3]). Therefore $\det(M_\beta)$ and $\det(M_\phi)$ are in the same square class mod p . \square

We now introduce notation from [15, Section 2] and [9, Appendice A]. Let $p \neq \ell$ be primes such that $p \geq 3$. For an elliptic curve E/\mathbb{Q}_ℓ with potentially good reduction write $L = \mathbb{Q}_\ell^{\text{un}}(E[p])$. Write also $I = \text{Gal}(L/\mathbb{Q}_\ell^{\text{un}})$. Write \bar{E} for the elliptic curve over $\bar{\mathbb{F}}_\ell$ obtained by reduction of a minimal model of E/L and $\varphi: E[p] \rightarrow \bar{E}[p]$ for the reduction morphism which is a symplectic isomorphism of G_L -modules. Let $\text{Aut}(\bar{E})$ be the automorphism group of \bar{E} over $\bar{\mathbb{F}}_\ell$ and write $\psi: \text{Aut}(\bar{E}) \rightarrow \text{GL}(\bar{E}[p])$ for the natural injective morphism. The action of I on L induces an injective morphism $\gamma_E: I \rightarrow \text{Aut}(\bar{E})$. Moreover, for $\sigma \in I$ we have

$$(3.1) \quad \varphi \circ \bar{\rho}_{E,p}(\sigma) = \psi(\gamma_E(\sigma)) \circ \varphi.$$

The following group theoretical lemma is proved in Section 3.1. For convenience we state it here since it plays a crucial rôle in the proof of Theorem 4.

Lemma 2. *Let $p \geq 3$ and $G = \text{GL}_2(\mathbb{F}_p)$. Let $H \subset \text{SL}_2(\mathbb{F}_p) \subset G$ be a subgroup isomorphic to $\text{SL}_2(\mathbb{F}_3)$. Then the group $\text{Aut}(H)$ of automorphisms of H satisfies*

$$N_G(H)/C(G) \simeq \text{Aut}(H) \simeq S_4,$$

where $N_G(H)$ denotes the normalizer of H in G and $C(G)$ the center of G . Moreover,

- (a) if $(2/p) = 1$, then all the matrices in $N_G(H)$ have square determinant;
- (b) if $(2/p) = -1$, then the matrices in $N_G(H)$ with square determinant correspond to the subgroup of $\text{Aut}(H)$ isomorphic to A_4 .

Proof of Theorem 4. Let E, E' be elliptic curves as in the statement. Note that $L = \mathbb{Q}_2^{\text{un}}(E[p])$ is the smallest extension of \mathbb{Q}_2^{un} where E obtains good reduction and the reduction map φ is an isomorphism between the \mathbb{F}_p -vector spaces $E[p](L)$ and $\bar{E}[p](\bar{\mathbb{F}}_2)$. By hypothesis E' also has good reduction over L and the same is true for φ' . Applying equation (3.1) to both E and E' we see that $E[p]$ and $E'[p]$ are isomorphic I_2 -modules if we show that $\psi \circ \gamma_E$ and $\psi \circ \gamma_{E'}$ are isomorphic as representations into $\text{GL}(\bar{E}[p])$ and $\text{GL}(\bar{E}'[p])$, respectively.

We have that $j(\bar{E}) = j(\bar{E}') = 0$ (see the proof of [6, Theorem 3.2]) thus E and E' are isomorphic over $\bar{\mathbb{F}}_\ell$. So we can fix minimal models of E/L and E'/L both reducing to the same \bar{E} . Write $H := \text{Aut}(\bar{E})$ and note that $H \simeq \text{SL}_2(\mathbb{F}_3)$ (see [16, Thm.III.10.1]). Therefore $\psi(\gamma_E(I)) = \psi(\gamma_{E'}(I)) = \psi(H) \subset \text{SL}(\bar{E}[p]) \subset \text{GL}(\bar{E}[p])$ and there must be an automorphism $\alpha \in \text{Aut}(\psi(H))$ such that $\psi(\gamma_E) = \alpha \circ \psi(\gamma_{E'})$. The first statement of Lemma 2 shows there is $g \in \text{GL}(\bar{E}[p])$ such that $\alpha(x) = gxg^{-1}$ for all $x \in \psi(H)$; thus $\psi \circ \gamma_E$ and $\psi \circ \gamma_{E'}$ are isomorphic representations.

Fix a symplectic basis of $\bar{E}[p]$ identifying $\text{GL}(\bar{E}[p])$ with $\text{GL}_2(\mathbb{F}_p)$. Let M_g denote the matrix representing g and observe that $M_g \in N_{\text{GL}_2(\mathbb{F}_p)}(\psi(H))$. Lift the fixed basis to bases of $E[p]$ and $E'[p]$ via the corresponding reduction maps φ and φ' . The lifted bases are symplectic. Write M_φ and $M_{\varphi'}$ for the matrices representing φ and φ' on these bases, respectively.

Set $M := M_{\varphi'}^{-1} M_g M_{\varphi}$. From (3.1) it follows that $\bar{\rho}_{E,p}(\sigma) = M^{-1} \bar{\rho}_{E',p}(\sigma) M$ for all $\sigma \in I$. Moreover, M represents some I_2 -modules isomorphism $\phi : E[p] \rightarrow E'[p]$ and from Lemma 1 we have that $E[p]$ and $E'[p]$ are symplectically isomorphic if and only if $\det(M)$ is a square mod p . Since φ and φ' are symplectic isomorphisms of G_L -modules Lemma 1 implies the determinants of M_{φ} and $M_{\varphi'}$ are squares mod p . Therefore $E[p]$ and $E'[p]$ are symplectically isomorphic if and only if $\det(M_g)$ is a square mod p .

Part (1) now follows from Lemma 2 (a).

We now prove (2). From Lemma 2 (b) we see that $E[p]$ and $E'[p]$ are symplectically isomorphic if and only if α is an automorphism in $A_4 \subset \text{Aut}(\psi(H)) \simeq S_4$. Note that these are precisely the inner automorphisms. For each p the map $\alpha_p := \psi^{-1} \circ \alpha \circ \psi$ defines an automorphism of $\gamma_E(I) = H = \text{Aut}(\bar{E})$ satisfying $\alpha_p \circ \gamma_{E'} = \gamma_E$. Since $\gamma_E, \gamma_{E'}$ are surjective and independent of p it follows that α_p is the same for all p . Since α and α_p are simultaneously inner or not it follows this property is independent of the prime p satisfying $(2/p) = -1$. This shows that $E[p]$ and $E'[p]$ are symplectically isomorphic I_2 -modules if and only if $E[\ell]$ and $E'[\ell]$ are symplectically isomorphic I_2 -modules for one (hence all) ℓ satisfying $(2/\ell) = -1$.

We are left to show that symplecticity is equivalent to $v_2(\Delta_m(E)) \equiv v_2(\Delta_m(E')) \pmod{3}$.

Since $(2/3) = -1$ from the observation above we can work with $p = 3$.

Fix $\omega \in \bar{\mathbb{F}}_2$ a primitive cubic root of unity. Let $L_3 \subset L$ be an extension of \mathbb{Q}_2^{un} of degree 8. Hence L/L_3 is cyclic of degree 3 and we write σ for a generator of $G = \text{Gal}(L/L_3) \subset I$. Thus $\gamma_E(G)$ and $\gamma_{E'}(G)$ are order 3 subgroups of $\text{Aut}(\bar{E})$.

Recall that $\psi : \text{Aut}(\bar{E}) \rightarrow \text{GL}(\bar{E}[3])$ is the natural injective morphism. After fixing a symplectic basis for $\bar{E}[3]$, conjugation by an element of $\text{SL}_2(\mathbb{F}_3)$ (which preserves the property of a basis of $\bar{E}[3]$ being symplectic) allows to assume that $\psi(\gamma_E(G))$ is the group generated by $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. In particular, E has a 3-torsion point defined over L_3 .

By doing the same for E' we obtain $\psi(\gamma_{E'}(\sigma)) = M_g \psi(\gamma_E(\sigma)) M_g^{-1}$, where M_g belongs to the normalizer $N = N_{\text{GL}_2(\mathbb{F}_3)}(\psi(\gamma_E(G)))$. Since the centralizer of $\psi(\gamma_E(\sigma))$ consists precisely of the elements of N with square determinant it follows that

$$\gamma_E(\sigma) = \gamma_{E'}(\sigma) \Leftrightarrow E[3] \simeq E'[3] \text{ symplectically.}$$

We can further assume that the residual curve \bar{E} is of the following form

$$\bar{E} : y^2 + a_3 y = x^3 + a_4 x + a_6, \quad a_i \in \bar{\mathbb{F}}_2, \quad a_3 \neq 0.$$

For such a model the elements of order 3 in $\text{Aut}(\bar{E})$ are the linear transformations $T(u) : (x, y) \mapsto (u^2 x, u^3 y)$, where $u = \omega^k$ for $k = 0, 1, 2$. Since E has a 3-torsion point defined over L_3 , the same argument leading to equation (17) in [9] applies (possibly after replacing σ by σ^2). Thus $\gamma_E(\sigma) = T(\omega^{v(\Delta_m(E))})$. By doing the same for E' we get $\gamma_{E'}(\sigma) = T(\omega^{v(\Delta_m(E'))})$ and the result follows. \square

3.1. A lemma in group theory. Write S_n and A_n for the symmetric and alternating group on n elements, respectively. We write $C(G)$ for the center of a group G . If H is a subgroup of G , then we write $N_G(H)$ for its normalizer and $C_G(H)$ for its centralizer in G .

Lemma 3. *Let $p \geq 3$ and $G = \mathrm{GL}_2(\mathbb{F}_p)$. Let $H \subset \mathrm{SL}_2(\mathbb{F}_p) \subset G$ be a subgroup isomorphic to $\mathrm{SL}_2(\mathbb{F}_3)$. Then the group $\mathrm{Aut}(H)$ of automorphisms of H satisfies*

$$N_G(H)/C(G) \simeq \mathrm{Aut}(H) \simeq S_4.$$

Moreover,

- (a) *if $(2/p) = 1$, then all the matrices in $N_G(H)$ have square determinant;*
- (b) *if $(2/p) = -1$, then the matrices in $N_G(H)$ with square determinant correspond to the subgroup of $\mathrm{Aut}(H)$ isomorphic to A_4 .*

Proof. We can write H as $H = \langle i, j, k, u \rangle$ where

- (1) $H_8 = \langle i, j, k \rangle$ is a subgroup isomorphic to the quaternion group; there is no other subgroup of H with order 8, hence H_8 is normal in H ;
- (2) u has order 3 and satisfies $uiu^{-1} = j$, $uju^{-1} = k$, $uku^{-1} = i$.

Let $\alpha, \beta \in \mathbb{F}_p^\times$ satisfy $\alpha^2 + \beta^2 = -1$ and consider the following elements of $\mathrm{SL}_2(\mathbb{F}_p) \subset G$

$$g_1 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad g_2 = \begin{pmatrix} \alpha & \beta \\ \beta & -\alpha \end{pmatrix}, \quad g_3 = \frac{1}{2} \begin{pmatrix} \alpha + \beta - 1 & \beta - \alpha - 1 \\ \beta - \alpha + 1 & -\alpha - \beta - 1 \end{pmatrix}.$$

It is known that H_8 can be conjugated by an element $g \in G$ into $\langle g_1, g_2 \rangle$. Moreover, we have $gHg^{-1} = \langle g_1, g_2, -g_1g_2, u_g \rangle$ where $gig^{-1} = g_1$, $g_jg^{-1} = g_2$, $gkg^{-1} = -g_1g_2$, $u_g = gu_g^{-1}$. One checks that the action by conjugation of u_g and g_3 on $\langle g_1, g_2 \rangle$ is equal, therefore $u_g = g_3\lambda$ for some scalar matrix λ . Since $u_g \in \mathrm{SL}_2(\mathbb{F}_p)$ by taking determinants we see that $\lambda = \pm 1$; $\lambda = -1$ is impossible due to order considerations, thus $u_g = g_3$. We have shown that we can suppose the generators of H are $i = g_1$, $j = g_2$, $k = -g_1g_2$ and $u = g_3$.

From [9, Lemma A.3] we have $C_G(H) = C(G)$. Now the action by conjugation induces a canonical group homomorphism $N_G(H) \rightarrow \mathrm{Aut}(H)$ with kernel $C_G(H)$, leading to an injection $N_G(H)/C(G) \rightarrow \mathrm{Aut}(H)$. To see that this map is also surjective (and hence an isomorphism), note that $N_G(H)$ contains the matrices

$$n_1 = \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} \quad \text{and} \quad n_2 = \begin{pmatrix} \alpha & \beta - 1 \\ \beta + 1 & -\alpha \end{pmatrix}$$

and that the subgroup of $N_G(H)/C(G)$ generated by the images of H and of these matrices has order 24. Since it can be easily checked that $\mathrm{Aut}(\mathrm{SL}_2(\mathbb{F}_3)) \simeq S_4$, the first claim follows.

Note that A_4 is the unique subgroup of S_4 of index 2. The determinant induces a homomorphism $S_4 \simeq N_G(H)/C(G) \rightarrow \mathbb{F}_p^\times/\mathbb{F}_p^{\times 2}$ whose kernel is either S_4 or A_4 . Since $H \subset \mathrm{SL}_2(\mathbb{F}_p)$ and all matrices in $C(G)$ have square determinant, it remains to compute $\det(n_1)$ and $\det(n_2)$. But $\det(n_1) = 2$ and $\det(n_2) = -\alpha^2 - (\beta - 1)(\beta + 1) = -\alpha^2 - \beta^2 + 1 = 2$ as well. \square

REFERENCES

- [1] S. Anni and S. Siksek, *On the generalized Fermat equation $x^{2\ell} + y^{2m} = z^p$ for $3 \leq p \leq 13$* , Preprint. [1](#)
- [2] I. Chen and S. Siksek, *Perfect powers expressible as sums of two cubes*, Journal of Algebra **322** (2009), 638-656. [1](#), [2](#)
- [3] H. Darmon. *Faltings plus epsilon, Wiles plus epsilon, and the generalized Fermat equation*, C. R. Math. Rep. Acad. Sci. Canada **19** (1), 1997 pp. 3-14. [1](#)

- [4] H. Darmon. *The equation $x^4 - y^4 = z^p$* , C. R. Math. Rep. Acad. Sci. Canada. **XV** (1993), no. 6, 286–290. [1](#)
- [5] H. Darmon and L. Merel, *Winding quotients and some variants of Fermat’s Last Theorem*, J. Reine Angew. Math. **490** (1997), 81–100. [1](#)
- [6] T. Dokchitser and V. Dokchitser, *Local invariants of isogenous elliptic curves*, Trans. Amer. Math. Soc. **367** (2015), no. 6, 4339–4358. [3](#)
- [7] N. Freitas, *Recipes for Fermat-type equations of the form $x^r + y^r = Cz^p$* , Math. Z. **279** (2015), no. 3-4, 605–639. [1](#)
- [8] N. Freitas, B. Naskręcki and M. Stoll, *The Generalized Fermat equation with exponents $2, 3, n$* . (in preparation) [1](#)
- [9] E. Halberstadt and A. Kraus, *Courbes de Fermat: résultats et problèmes*, J. Reine Angew. Math. **548** (2002), 167–234. [1](#), [2](#), [3](#), [3](#), [3.1](#)
- [10] A. Kraus, *Sur l’équation $a^3 + b^3 = c^p$* , Experimental Math. **7** (1998), no. 4, 1–13. [1](#), [1](#), [2](#)
- [11] A. Kraus, *Sur le défaut de semi-stabilité des courbes elliptiques à réduction additive*, Manuscripta Math. **69** (1990), no. 4, 353–385. [2](#)
- [12] A. Kraus and J. Oesterlé *Sur une question de B. Mazur*, Math. Ann. **293** (1992), 259–275 [1](#), [2](#)
- [13] I. Papadopoulos, *Sur la classification de Néron des courbes elliptiques en caractéristique résiduelle 2 et 3*, J. Number Theory, **44** (1993), no. 2, 119–152. [2](#)
- [14] B. Poonen, E. F. Schaefer and M. Stoll, *Twists of $X(7)$ and primitive solutions to $x^2 + y^3 = z^7$* , Duke Math. J. **137** (2007), no. 1, 103–158. [1](#)
- [15] J.-P. Serre and J. Tate, *Good reduction of abelian varieties*, Annals of Math. **88** (1968), no. 2, 492–517. [3](#)
- [16] J. H. Silverman, *The arithmetic of elliptic curves*, Second Edition, Graduate Texts in Mathematics **106**, Springer, Dordrecht, 2009. [3](#)
- [17] A. Wiles, *Modular elliptic curves and Fermat’s Last Theorem*, Annals of Math. **141** (1995), 443–551. [1](#)